



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/921,677

08/03/2001

Lee P. Noehring

2551-0052

8166

42624

7590

04/21/2009

DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

EXAMINER

THAI, HANH B

ART UNIT

PAPER NUMBER

2163

MAIL DATE

DELIVERY MODE

04/21/2009

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte LEE P. NOEHRING, CHAD W. MERCER, and STEVE J.
BROWN

Appeal 2008-3261
Application 09/921,677
Technology Center 2100

Decided: April 21, 2009

Before JOHN C. MARTIN, LANCE LEONARD BARRY, and CAROLYN
D. THOMAS, *Administrative Patent Judges*.

BARRY, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

The Patent Examiner rejected claims 10-18 and 35. The Appellants appeal therefrom under 35 U.S.C. § 134(a). We have jurisdiction under 35 U.S.C. § 6(b).

INVENTION

The invention at issue on appeal uses a first-come, first-serve scheme to update entries in a security association database ("SAD") by selectively granting access to security channels that need to update the same SAD. (Spec. 3-4.)

ILLUSTRATIVE CLAIM

10. In a system having multiple security channels, a method of modifying an entry in a security association database, the method associated with each channel comprising:

- requesting access to a predetermined address location in the security association database;

- assigning a weight value to the request based on a sequential order of the request relative to access requests to the predetermined address location made by other of the security channels;

- retrieving the security association data structure from the predetermined address location when, based on the weight value assigned to the request, the channel has a higher priority request relative to the other security channel requests;

- modifying the retrieved security association data structure; and

- writing the modified security association data structure to the predetermined address location in the security association database.

PRIOR ART

Baker	US 5,948,080	Sep. 7, 1999
Bryers	US 2003/0126233 A1	Jul. 2, 2003
Vange	US 2002/0002618 A1	Jan. 3, 2002 (Filed Apr. 16, 2001)

REJECTIONS

Claims 10-14, 16, 17, and 35 stand rejected under 35 U.S.C. § 103(a) as being obvious over Bryers and Vange.

Claims 15 and 18 stand rejected under § 103(a) as being obvious over Bryers, Vange, and Baker.

ISSUE

"Rather than reiterate the positions of parties *in toto*, we focus on the issue therebetween." *Ex parte Filatov*, No. 2006-1160, 2007 WL 1317144, at *2 (BPAI Apr. 20, 2007). The Examiner makes the following findings.

Bryers clearly discloses requesting access to a predetermined address location in the security association database ([0286]-[0287], Bryers); a weight value for priority level of the security channels ([0178]-[0183] and [0581]-[0588], Bryers discloses a weight value of the packet's priority); retrieving the security association data structure from the predetermined address location ([0194]; [0195] and [0198]

(Ans. 8.) She also finds that "Vange discloses the shared bandwidth amongst a plurality of users on a first-in first-out basis (§[0007])" (citation omitted) (*Id.*). The Appellants argue that "these references fail to disclose or

suggest at least assigning a weight value to the request based on a sequential order of the request relative to access requests to the predetermined address location made by other of the security channels." (Amended App. Br. 6.)

Therefore, the issue before us is whether the Appellants have shown error in the Examiner's finding that Bryers and Vange would have suggested assigning a weighting value to a security channel's request to access a predetermined address location in a security association database to order requests made by a plurality of security channels.

LAW

The question of obviousness is "based on underlying factual determinations including . . . what th[e] prior art teaches explicitly and inherently" *In re Zurko*, 258 F.3d 1379, 1383-1384 (Fed. Cir. 2001) (citing *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966); *In re Dembiczak*, 175 F.3d 994, 998 (Fed. Cir. 1999); *In re Napier*, 55 F.3d 610, 613 (Fed. Cir. 1995)).

FINDINGS OF FACT ("FFs")

1. [Bryers' Internet Protocol Security]

IPSec module operates as generally shown in FIG. 10. As each new packet enters the IPSec module at 1010, a determination is made as to whether the packet needs to be encapsulated at step 1016 or de-capsulated at step 1012. If the packet is an encapsulation case, at step 1014, the system will extract the security parameter index (SPI) and do an anti replay check. Basic firewall rules will be applied based on the tunneling [Internet Protocol] IP. The security association (SA) will be retrieved from the security association database, and the packet de-capsulated using the security association.

The internal header will be cross-checked with the security association. The security association status will be updated and renewal triggered if needed.

(¶ 0194.)

2. The same references' first tier "cache 2052 determines whether to select a memory access request from [central processing unit] CPU 2060, coprocessor 2062, or second tier cache 2080. In one embodiment, cache 2052 gives cache 2080 the highest priority and toggles between selecting the CPU and coprocessor." (¶ 0286.)

3. Bryers' "[b]andwidth allocation circuit 3134 (FIG. 41) monitors traffic flowing through sink port 3052 and manages the bandwidth allocated to different data packet priority levels." (¶ 0581.) The "[s]ink port 3052 and multi-sink port 3112 are configured to have a Priority Weighting Value ('PWV') for each priority level." (citation omitted) (¶ 0585.)

4. Vange includes the following disclosure.

Users connect to the Internet through a variety of mechanisms, but many mechanisms use shared bandwidth connections. For example, data connections using broadband wireless access (BWA), cellular telephones and cable modems typically share a given amount of bandwidth amongst a plurality of users. Each user's data is transported on a first-in first-out (FIFO) basis.

(¶ 0007.)

ANALYSIS

Bryers is a large reference, and the Examiner's rejection relies on disparate and distinct parts thereof. One part explains that an IPSec module retrieves data from a security association database and updates the security association. (FF 1.) The Examiner has not shown that the reference assigns a weighting value to a request from the IPSec module to access a predetermined address location in the security association database. Nor has she alleged, let alone shown, that the IPSec module features a plurality of security channels making requests to access the database such that such assignments would have been desirable.

Another part of Bryers discusses a first tier cache granting priority to access requests from a CPU, a coprocessor, and a second tier cache. (FF 2.) The first tier data cache, however, is not the reference's aforementioned security association database. Nor is the CPU, coprocessor, or second tier cache tantamount to the IPSec module, which is the module that accesses the security association database.

Still another part of Bryers discloses configuring sink ports to have a Priority Weighting Value for each priority level of data traffic. (FF 3.) We agree with the Appellants that this part relates to "determin[ing] a set of distributed target bandwidths for a plurality of traffic classes, to thereby allow the content aggregator to provide bandwidth guarantees for the system as a whole. Traffic classes are predefined, and when packets arrive each is classified to determine in which traffic class it belongs." (Amended Appeal Br. 4-5.) Configuring sink ports is not tantamount to assigning a weighting

value to a security channel's request to access a predetermined address location in a security association database.

For its part, Vange merely discloses that many users who connect to the Internet share bandwidth connections. Such a connection transports each user's data on a FIFO basis. (FF 4.) Connecting users to the Internet is not tantamount to connecting security channels to a predetermined address location in a security association database. Furthermore, transporting data from users in a FIFO basis is not tantamount to assigning a weighting value to a security channel's request to access a predetermined address location in a security association database to order requests made by a plurality of security channels.

The Examiner does not allege, let alone show, that the addition of Baker cures the aforementioned deficiency of Bryers and Vange.

CONCLUSION

Based on the aforementioned facts and analysis, we conclude that the Appellants have shown error in the Examiner's finding that Bryers and Vange would have suggested assigning a weighting value to a security channel's request to access a predetermined address location in a security association database to order requests made by a plurality of security channels.

ORDER

We reverse the rejections of claims 10-18 and 35.

Appeal 2008-3261
Application 09/921,677

REVERSED

erc

DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON VA 22203